# 使用身份服務(IdS)的CCE單一登入故障排除 — 證書管理

## 目錄



## 簡介

本文檔介紹在UCCE/PCCE中重新生成和交換SAML證書的詳細步驟，以確保安全、清晰的流程。


作者：Nagarajan Paramasivam，思科TAC工程師。


## 必要條件

### 需求

思科建議您瞭解以下主題：

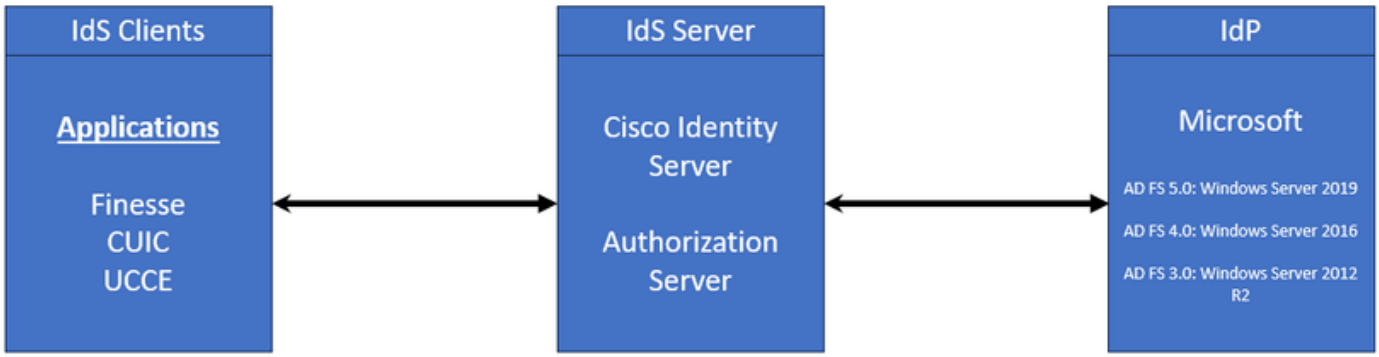
- 套裝/整合客服中心企業版(PCCE/UCCE)
- 語音作業系統(VOS)平台
- 憑證管理
- 安全斷言標籤語言(SAML)
- 安全通訊端層 (SSL)

- Active Directory聯合身份驗證服務(AD FS)
- 單一登入(SSO)

### 採用元件

本檔案中的資訊是根據以下元件：

- 思科身分識別服務（思科IdS）
- 身份提供程式(IdP)- Microsoft Windows ADFS




本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

在UCCE/PCCE中，思科身份服務(Cisco IdS)提供身份提供者(IdP)和應用之間的授權。

配置思科IdS時，您可以在思科IdS和IdP之間設定後設資料交換。此交換建立了信任關係，然後允許應用程式使用思科Id進行SSO。您可以從Cisco IdS下載後設資料檔案並將其上傳到IdP，從而建立信任關係。

SAML證書與SSL證書類似，在某些情況下需要更新或更改它。在Cisco Identity Services(IdS)伺服器上重新生成或交換SAML證書時，可能導致與身份提供程式(IdP)的受信任連線中斷。 此中斷可能導致依賴單一登入的客戶或使用者無法獲得訪問系統所需的授權的問題。

本文檔旨在介紹各種常見情況，在這些情況下，您必須在Cisco IdS伺服器上建立新的SAML證書。還說明如何將此新證書提供給身份提供方(IdP)，以便重建信任。這樣，客戶端和使用者就可以繼續使用單一登入而不出現任何問題。目標是確保您擁有順利進行憑證更新程式所需的所有資訊，而不會產生混淆。

需牢記的要點：

1. SAML證書預設情況下在Cisco IdS伺服器安裝期間生成，有效期為3年

2. SAML證書是自簽名證書

3. SAML證書是駐留在Cisco IDS發佈者和訂閱者上的SSL證書

4.只能在Cisco IDS Publisher節點中執行SAML證書重新生成

5. SAML證書的安全雜湊演算法的可用型別是SHA-1和SHA-256

6. SHA-1演算法用於IdS 11.6，而在以前的版本中，SHA-256演算法用於IdS 12.0及更高版本

7.身份提供程式(IdP)和身份服務(IdS)都必須使用相同的演算法型別。

8.只能從Cisco IdS Publisher節點(sp-<Cisco IdS_FQDN>.xml)下載Cisco IdS SAML證書

9.請參閱此連結瞭解UCCE/PCCE單點登入配置。UCCE 12.6.1功能指南

# SAML證書已過期

SAML證書的生成具有3年（1095天）的有效期，並且必須在到期之前更新SAML證書。過期的SSL證書被視為無效證書，它會破壞思科身份服務(IdS)和身份提供程式(IdP)之間的證書鏈。

# 解決方案

1.檢查SAML證書到期日期

2.重新生成SAML證書

3.下載sp.xml檔案

4.從sp.xml檔案中檢索SAML證書

5.將舊的SAML證書替換為IdP中的新SAML證書

6.有關詳細步驟，請參閱參考部分

---

(注意: {由於只更改了SAML證書，因此不需要將IdS後設資料交換為IdP})

---

# 身份提供程式(IdP)中的安全雜湊演算法更改

假設在採用單點登入的現有PCCE/UCCE環境中。IdP和Cisco IdS伺服器均配置了SHA-1安全雜湊演算法。考慮到SHA-1的弱點需要將安全雜湊演算法更改為SHA-256。

# 解決方案

1.更改AD FS信賴信任方中的安全雜湊演算法（SHA-1更改為SHA-256）

2.將IdS發佈伺服器中的安全雜湊演算法更改為金鑰和證書（SHA-1更改為SHA-256）

3.在IdS發佈器中重新生成SAML證書

4.下載sp.xml檔案

5.從sp.xml檔案中檢索SAML證書

6.將舊的SAML證書替換為IdP中的新SAML證書

7.有關詳細步驟，請參閱參考部分

## Cisco IdS伺服器IP地址或主機名更改 — 重建了共存的CUIC/LiveData/IdS發佈伺服器或獨立IdS發佈伺服器 — 重建了共存的CUIC/LiveData/IdS訂閱伺服器或獨立IdS訂閱伺服器

這些情況很少發生，強烈建議重新開始採用單點登入(SSO)設定，以確保生產環境中的SSO功能得到及時而有效的恢復。必須優先安排此重新配置，以儘量減少對使用者所依賴的SSO服務的中斷。

## 解決方案

1.從AD FS中刪除現有信賴方

2.上傳Cisco IdS伺服器tomcat信任中的AD FS SSL證書

3.下載sp.xml檔案

4.有關詳細步驟，請參閱「參考」一節和「功能指南」

5.在AD FS中配置信賴信任方

6.新增索賠規則

7.啟用簽名的SAML斷言

8.下載AD FS聯合後設資料

9.將聯合後設資料上傳到Cisco IdS伺服器

10.執行測試SSO

## 參考

如何在ADFS或

## 如何啟用簽名的SAML斷言

如需詳細步驟，請參閱以下檔案：UCCE 12.6.1功能指南

## 如何將AD FS SSL證書上傳到Cisco IdS tomcat信任

1.下載或檢索AD FS SSL證書

2.訪問Cisco IdS Publisher OS管理頁面

3.使用作業系統管理員憑據登入

4.定位至「安全性」>「證書管理」

5.按一下「Upload Certificate/Certificate Chain」，系統就會開啟快顯視窗

6.按一下「下拉選單」，然後在「證書用途」上選擇tomcat-trust

7.按一下瀏覽並選擇AD FS SSL證書

8.按一下「上傳」

---

(附註：{信任證書會複製到訂閱伺服器節點。您不需要上載到訂閱伺服器節點。})

---

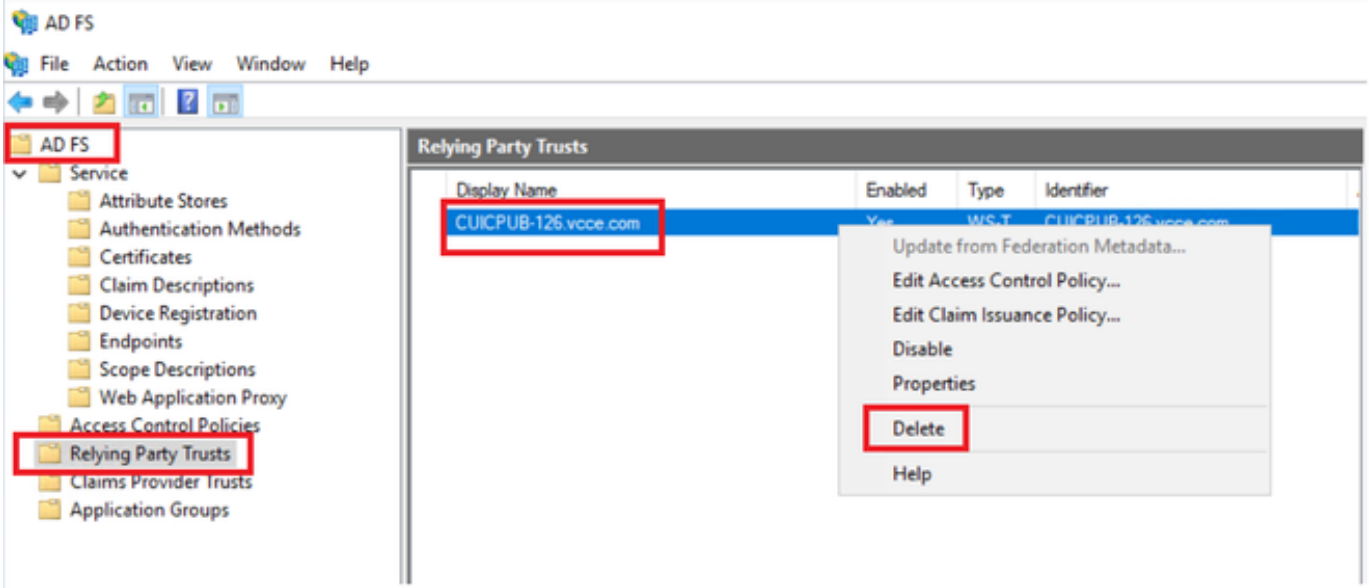
## 如何刪除AD FS中的信賴方

1.使用管理員特權憑據登入到身份提供程式(IdP)伺服器

2.開啟「伺服器管理器」，然後選擇「AD FS」>「工具」>「AD FS管理」

3.在左側樹中，選擇AD FS下的信賴方信任

4.按一下右鍵Cisco IdS伺服器，然後選擇「刪除」




## 如何檢查或更改身份提供程式(IdP)中配置的安全雜湊演算法

1.使用管理員特權憑據登入到身份提供程式(IdP)伺服器

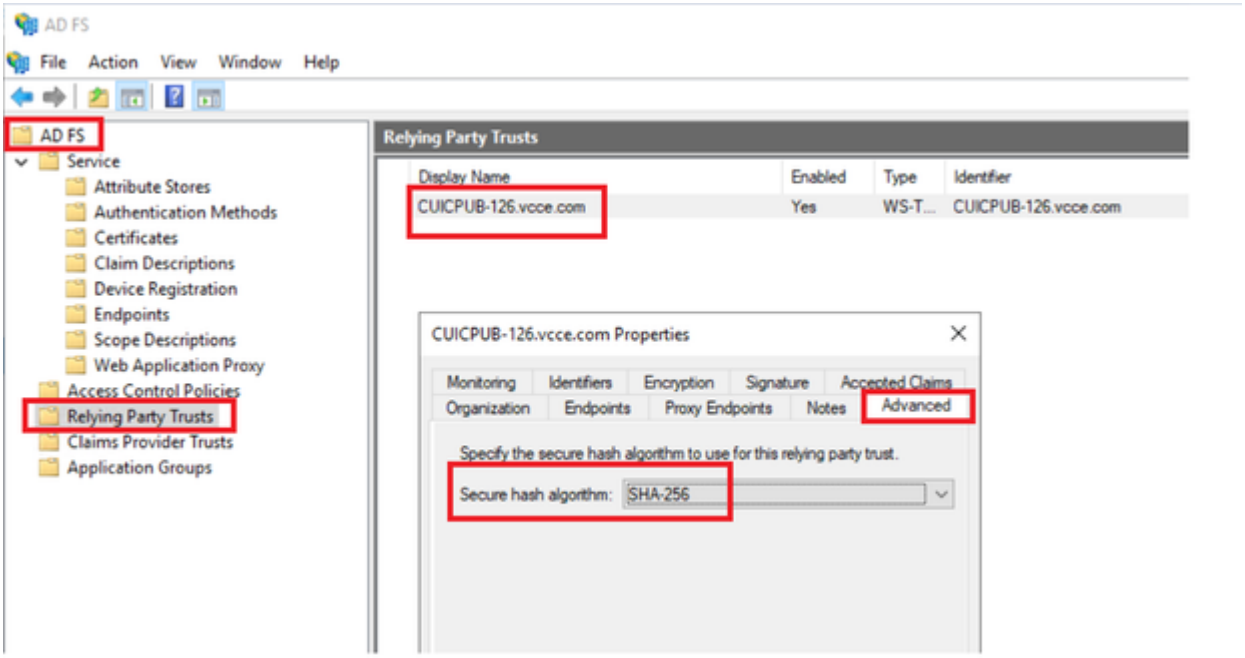
2.開啟「伺服器管理器」，然後選擇「AD FS」>「工具」>「AD FS管理」

3.在左側樹中，選擇AD FS下的信賴方信任

4.按一下右鍵Cisco IdS伺服器並選擇屬性

5.定位至「高級」標籤

6.安全雜湊演算法選項顯示AD FS伺服器中配置的安全雜湊演算法。



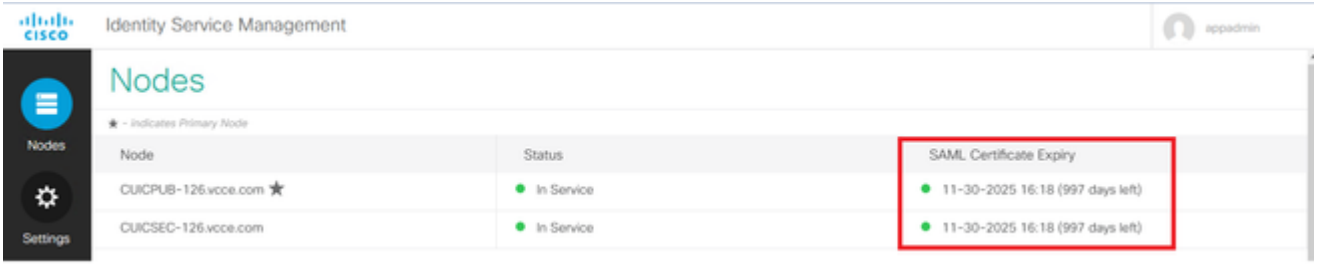
7.按一下「下拉選單」，然後選擇所需的安全雜湊演算法。

## 如何檢查Cisco IdS伺服器SAML證書到期日期

1.使用應用程式使用者憑據登入到Cisco IdS伺服器發佈伺服器或訂閱伺服器節點

2.成功登入後，頁面將轉至Identity Service Management > Nodes

3.顯示Cisco IdS發佈者和訂閱者節點、狀態和SAML證書到期




---

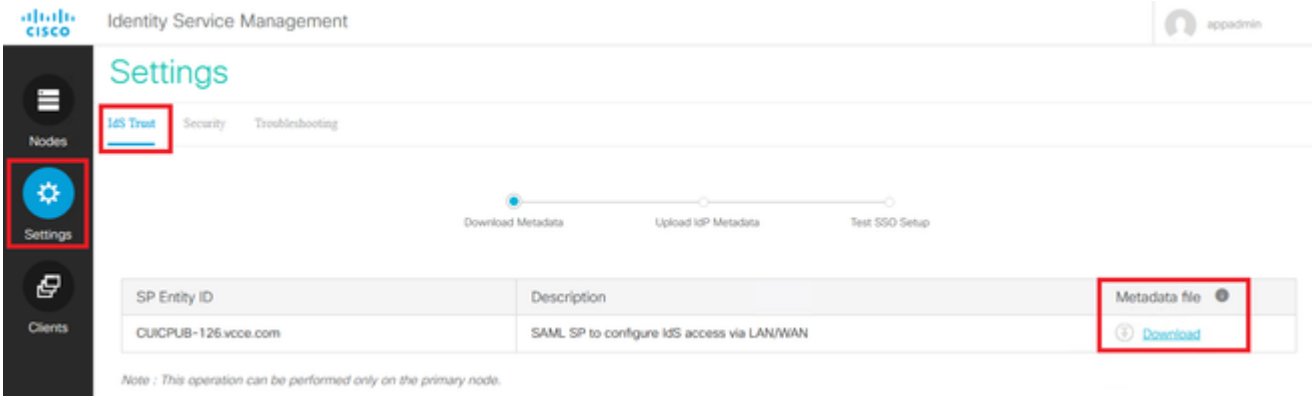
## 如何下載Cisco IdS伺服器的後設資料

1.使用應用程式使用者憑據登入到Cisco IdS Publisher節點

2.按一下「設定」圖示

3.定位至「IDS信任」標籤

4.按一下「下載」連結下載Cisco IdS群集的後設資料




## 如何從sp.xml檔案中檢索SAML證書

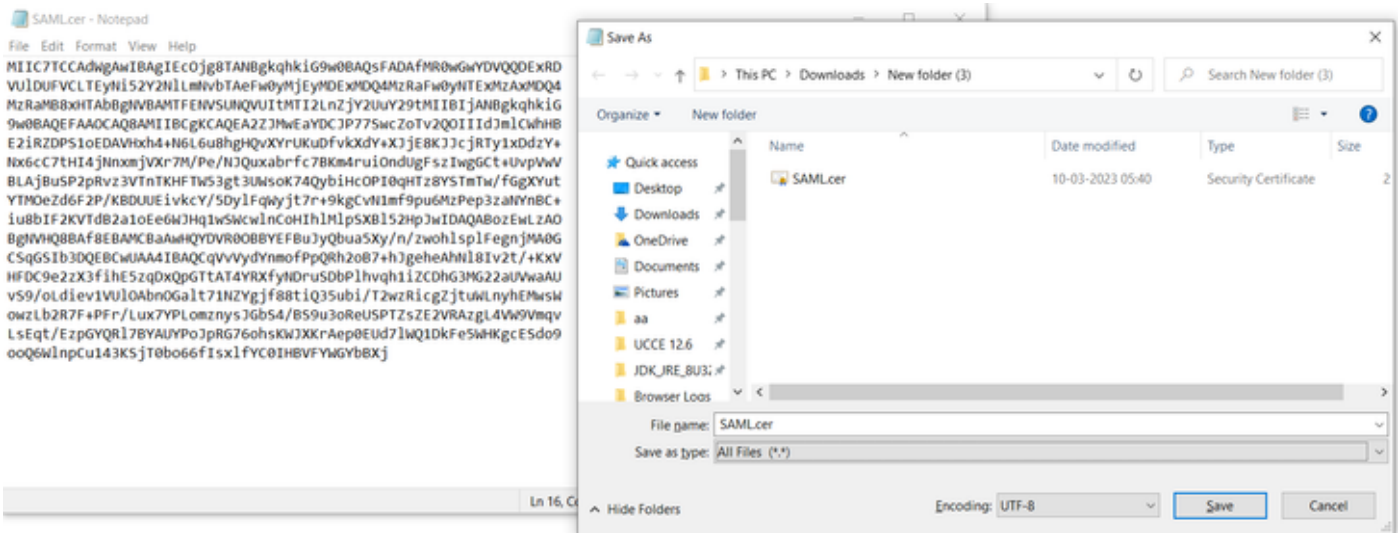
1.使用文本編輯器開啟sp.xml檔案

2.在標頭<ds:X509Certificate></ds:X509Certificate>之間複製原始資料

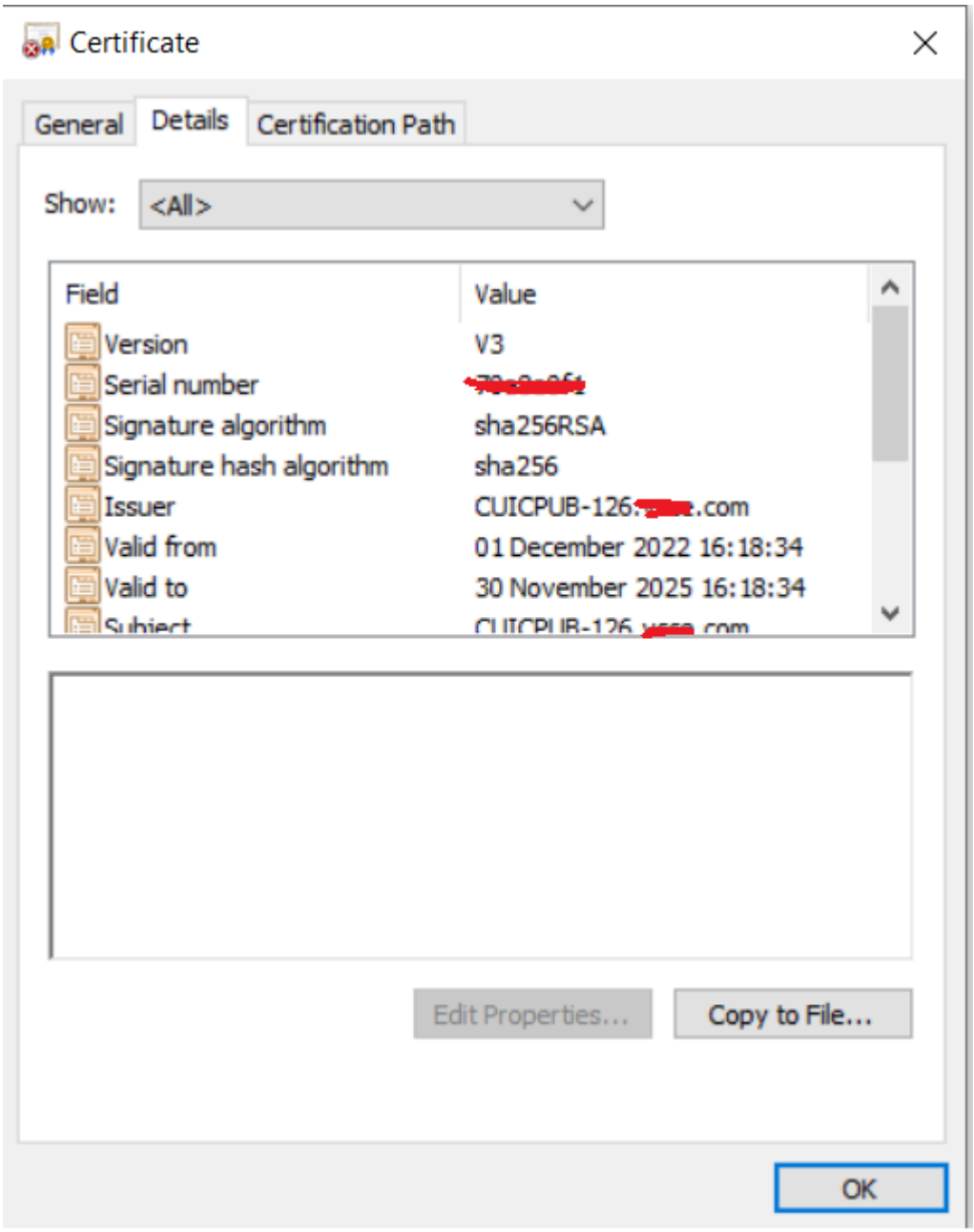
```
<ds:X509Certificate>MIIC7TCCAdWgAwIBAgIEcOjg8TANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDExRD
VUlDUFVCLTEyNi52Y2NlLmNvbTAeFw0yMjEyMDExMDQ4MzRaFw0yNTExMzAxMDQ4
MzRaMB8xHTAbBgNVBAMTFENVSUNQVUItMTI2LnZjY2UuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ZJMwEaYDCJP77SwcZoTv2QOIIIdJmlCWhHB
E2iRZDPS1oEDAVHxh4+N6L6u8hgHQvXYrUKuDfvkXdY+XJjE8KJJcjRTy1xDdzY+
Nx6cC7tHI4jNnxmjVXr7M/Pe/NJQuxabrfc7BKm4ruiOndUgFszIwgGCt+UvpVwV
BLAjBuSP2pRvz3VTnTKHFTW53gt3UWsoK74QybiHcOPI0qHTz8YSTmTw/fGgXYut
YTMOeZd6F2P/KBDUUEivkcY/5DylFqWyjt7r+9kgCvN1mf9pu6MzPep3zaNYnBC+
iu8bIF2KVTdB2a1oEe6WJHq1wSWcwlnCoHIhlMlpSXBl52HpJwIDAQABozEwLzAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0OBBYEFBuJyQbua5Xy/n/zwohlsplFegnjMA0G
CSqGSIb3DQEBCwUAA4IBAQCqVvVydYnmofPpQRh2oB7+hJgeheAhNl8Iv2t/+KxV
HFDC9e2zX3fihE5zqDxQpGTtAT4YRXfyNDruSDbPlhvqh1iZCDhG3MG22aUVwaAU
vS9/oLdiev1VUlOAbnOGalt71NZYgjf88tiQ35ubi/T2wzRicgZjtuWLnyhEMwsW
owzLb2R7F+PFr/Lux7YPLomznysJGbS4/BS9u3oReUSPTZsZE2VRAzgL4VW9Vmqv
LsEqt/EzpGYQRl7BYAUYPoJpRG76ohsKWJXKrAep0EUd7lWQ1DkFe5WHKgcESdo9
ooQ6WlnpCu143KSjT0bo66fIsxlfYC0IHBVFYWGYbBXj</ds:X509Certificate>
```

3.開啟另一個文本編輯器並貼上複製的資料

4.儲存檔案.CER格式




5.開啟證書以檢視證書資訊




## 如何替換AD FS中的SAML證書

1.將SAML證書檔案複製到從sp.xml檢索的AD FS伺服器

2.開啟「伺服器管理器」，然後選擇「AD FS」>「工具」>「AD FS管理」

3.在左側樹中，選擇AD FS下的信賴方信任

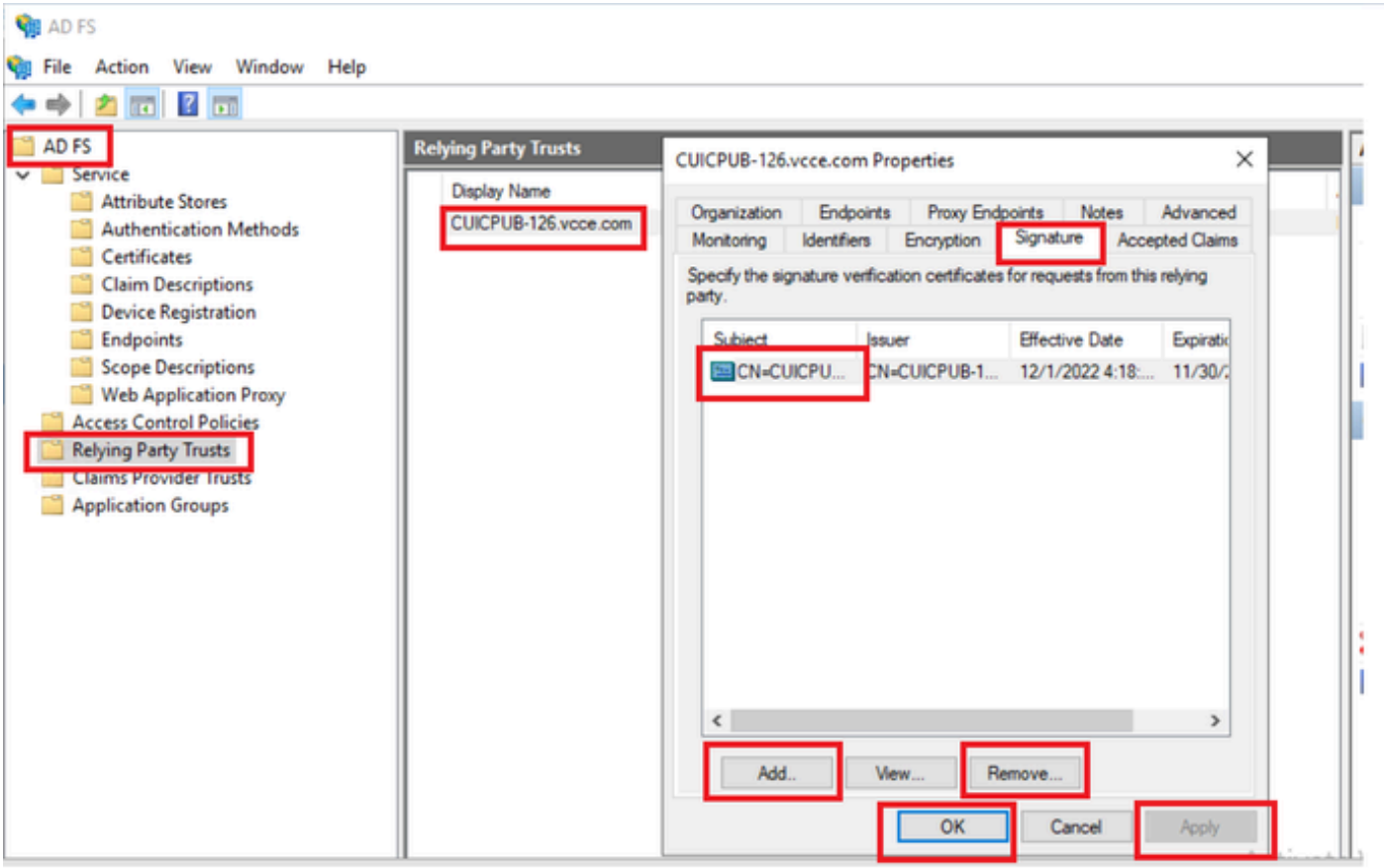
4.按一下右鍵Cisco IdS伺服器並選擇屬性

5.定位至「簽名」標籤

6.按一下新增並選擇新生成的SAML證書

7.選擇舊SAML證書，然後按一下「刪除」

8.應用和儲存




## 如何在Cisco IdS伺服器中重新生成SAML證書

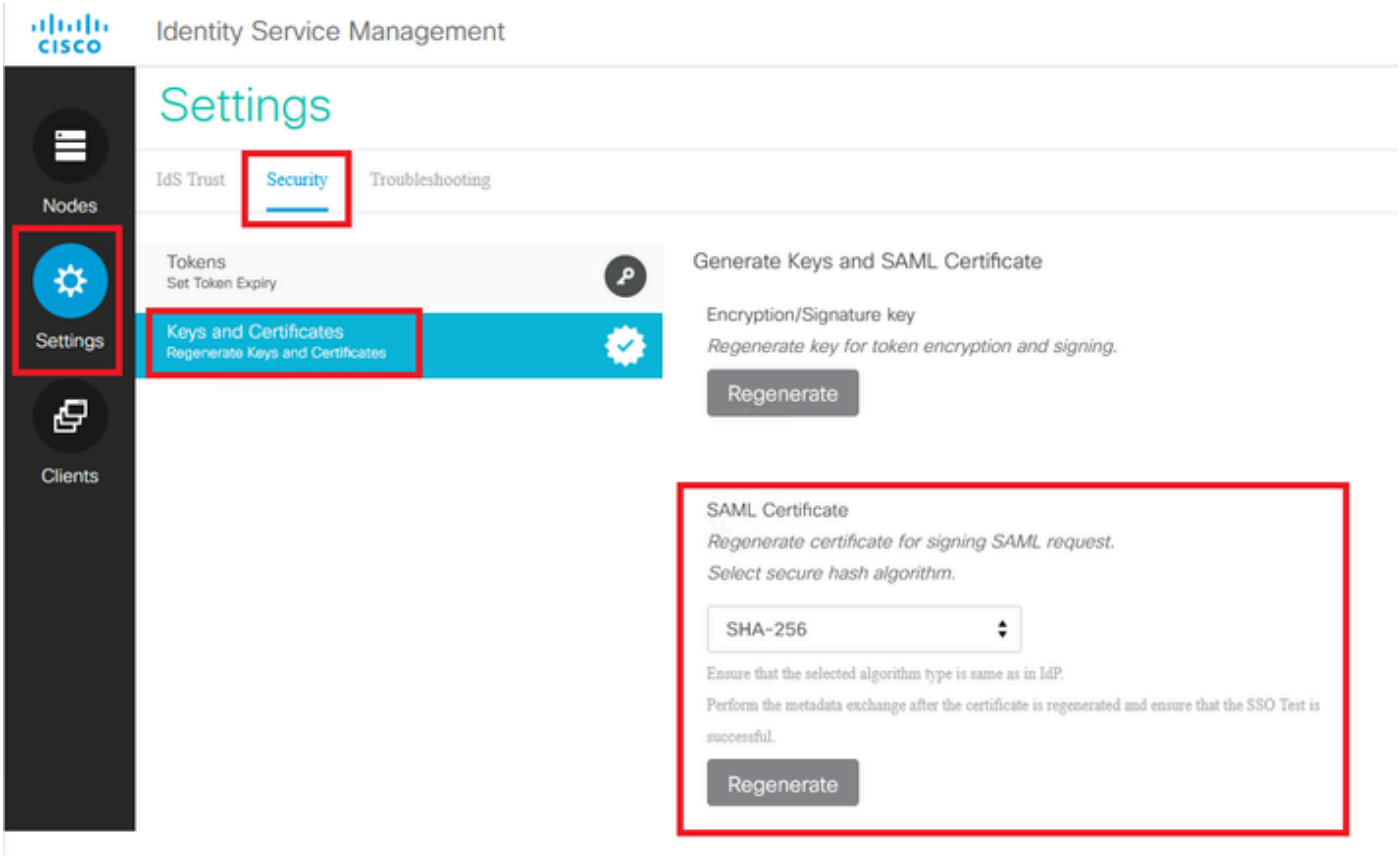
1.使用應用程式使用者憑據登入到Cisco IdS Publisher節點

2.按一下「設定」圖示

3.定位至「安全性」標籤

4.選擇「金鑰和證書」選項

5.點選SAML證書部分下的Regenerate按鈕（突出顯示）




## 測試SSO

每當SAML證書發生更改時，請確保TEST SSO在Cisco IdS伺服器中成功，並從CCEAdmin頁面重新註冊所有應用程式。

1.從承擔者AW伺服器訪問CCEAdmin頁

2.以管理員級別的許可權登入到CCEAdmin門戶

3.定位至「概覽」>「功能」>「單一登入」

4.點選Register with Cisco Identity Service下的Register按鈕

5.執行測試SSO

## Azure證書再生

1.從IDS重新生成證書（僅在發佈伺服器中），這將為發佈伺服器和訂閱伺服器自動生成證書
2.從IDS下載後設資料並上傳到IDP/Azure
3.從IDP/Azure續訂證書，這將完全更改Azure中的後設資料，並將從Microsoft Azure對其進行簽名，從而解決.pfx的需求
4.將後設資料從IDP/Azure上載到Cisco IDS（僅在發佈伺服器中）
5.從IDS測試SSO

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。